

- 1 -

METHOD AND DEVICE FOR THE GENERATION OF
CHECKABLE FORGERY-PROOF DOCUMENTS

Description:

The invention relates to a method for the generation of forgery-proof documents or data records, whereby key information is generated and encrypted checking information is formed from the key information and from a transaction indicator.

The invention also relates to a value transfer center and to a cryptographic module.

Numerous methods are known for generating forgery-proof documents and for checking them. Familiar methods are based on the generation of digital signatures or encrypted checking information, which are produced within the scope of the generation of the document.

A distinction has to be made between documents for which the writer has an interest in their genuineness and those for which third parties have an interest in their genuineness.

If a third party has an interest in documents being forgery-proof, then it is a known procedure to use a so-called "cryptographic module" for generating the document. Such known cryptographic modules are characterized in that they contain electronic data within them or that they process data that cannot be accessed or manipulated from the outside.

A cryptographic module can be regarded as a secure, sealed unit in which security-relevant processes are carried out that cannot be manipulated from the outside. A worldwide recognized standard for such cryptographic modules is the standard for cryptographic modules published under the designation FIPS Pub 140 by the United States National Institute of Standards and Technology – NIST.

If a cryptographic module is used to generate forgery-proof documents for which third parties have an interest in their genuineness, then a customary implementation is that the cryptographic module is used to securely deposit cryptographic keys that serve within the module, and only there, to encrypt check values. For example, so-called signature cards of the type issued by certification agencies or trust centers for generating digital signatures are a familiar approach. These signature cards, in the form of microprocessor chip cards, also contain a cryptographic module precisely in this microprocessor chip.

As a rule, one or more asymmetrical key pairs are deposited in such modules which are characterized in that encryptions that have been generated with the so-called private key can only be reversed with the associated public key, and in that encryptions that have been generated with the public key can only be reversed with the associated private key. As their name indicates, public keys are intended for public disclosure and widespread dissemination, whereas private keys may not be handed out and, when used together with cryptographic modules, they must not leave these modules at any point in time. Also deposited in such modules are algorithms, for example, for forming checksums or, in the example of the digital signature, for generating a so-called digital fingerprint or "hash value" which is characterized in that it maps any desired data contents onto generally quantitatively considerably abbreviated information in such a way that the result is irreversible and unambiguous and in that, for different data contents with which the algorithm is supplied, different results are obtained in each case.

The generation of a forgery-proof document in whose genuineness third parties have an interest, which is done by means of a cryptographic module containing asymmetrical keys and an algorithm to form check values, is generally carried out in the following manner: first of all, using the algorithm to form check values, a check value is formed that relates to the document that is to be secured. Then a private key in the cryptographic module is used to encrypt the check value. The combination of these two processes is referred to as the generation of a "digital signature".

The checking of such a digital signature is normally carried out as follows: the recipient receives the document and the encrypted check value. The recipient also needs – and this is the objective of the invention described below – the public key of the document producer and

the recipient uses this public key to decrypt the check value that the document producer has encrypted within the cryptographic module with his private key. Therefore, after the decryption, the recipient has the unencrypted check value. Moreover, in the next step, the recipient applies the same algorithm in order to form a check value for the received document. Finally, in the third step, the recipient compares the check value he himself has generated to the decrypted check value of the document producer. If both check values match, then the document was not forged and the genuineness of the document is substantiated beyond a doubt. Normally, in the case of known digital signatures, the authenticity of the document producer is checked. This is done in that the public key of the document producer is likewise digitally signed by a so-called certification agency or "CA" and it is allocated to a certain cryptographic module, or to a certain owner of the cryptographic module. In this case, the recipient of the document does not simply accept the public key of the document producer as a given but rather he likewise ascertains whether it belongs to the document producer by checking the digital signature of the public key in the manner described above.

With this known method, the problem exists that, in order to check the genuineness of a document, it is necessary to have information that is directly related to the document producer's use of keys by means of the cryptographic module. In the typical example described above for generating digital signatures, this is the public key of the document producer or of his cryptographic module, which has to be used for the checking procedure. In the case of the signature of the public key by a certification agency, the entire set comprising the public key, the identification of the user of this key and the digital signature of the certification agency is designated as the "key certificate".

To sum it up, this problem can be illustrated with reference to an example as follows: in order to check the genuineness of a normally digitally signed document, the public key or the key certificate of the document producer or of his cryptographic module has to be available during the checking procedure. If, as is customary, documents of different document producers are to be checked in a checking station, then it is necessary for all of the public keys or all of the key certificates of all document producers to be available there.

There are various ways to meet the requirement that the public key of the document producer has to be available during the checking procedure. Thus, it is possible to attach the public key

or the key certificate of the document producer to the document that is to be secured. Another possibility is to deposit the public key at the checking station and to access it as the need arises.

The known methods, however, are associated with drawbacks.

Attaching the key or the key certificate is disadvantageous if the size of the document has to be kept as small as possible and if an attached key would excessively enlarge the data record that is to be printed, transmitted or processed.

Depositing a public key at the checking station is especially disadvantageous if access to keys deposited at the checking station is not possible for practical or time reasons, for example, in case of a very large number of stored keys which would have to be accessed within a very short period of time.

In order to overcome these known disadvantages, with a method of this generic type, it is disclosed in this applicant's German patent specification DE 100 20 563 C2 to generate a secret in a security module, to transfer the secret together with information that reveals the identity of the security module in encrypted form to a certification agency, to decrypt the secret in the certification agency, thus recognizing the identity of the security module, to subsequently encrypt the secret together with information on the identity of the document producer in such a way that only a checking station can carry out a decryption, in order to then transmit the secret to a document producer. With this method, the document producer enters his own data into the security module, whereby the data entered by the document producer himself is irreversibly linked to the secret by means of the security module and whereby the secret cannot be reconstructed.

This known method is characterized in that the document that is transmitted to a checking station is formed from the result of the irreversible linking of the secret to the data entered by the document producer, from the data entered by the document producer himself and from the encrypted information of the certification agency.

This known method is especially suitable for generating and checking forgery-proof postage stamps of a postal service provider. Such postage stamps are generated by customers of a postal service provider using a personal cryptographic module and they are applied onto the mailpiece as a machine-readable barcode. The machine-readable barcode has only a very limited data scope and consequently, it does not allow the entry of the public key of the customer. Moreover, during the so-called letter production, the digital postage stamps have to be read and checked within a very short period of time, as a result of which the possibility of accessing a database containing perhaps many millions of public keys is likewise not an option.

The invention is based on the objective of further developing a known method in such a way that it can be carried out, independent of direct communication between the cryptographically reliable contact station and the document producer.

According to the invention, this objective is achieved in that the generation of the random key information and the formation of the encrypted checking information from the key information and from the transaction indicator are carried out in a cryptographically reliable contact station, in that the cryptographically reliable contact station encrypts the key information, and in that the encrypted checking information and the encrypted key information are transmitted by the cryptographically reliable contact station to an intermediate station, in that the intermediate station temporarily stores the encrypted key information and the encrypted checking information and transmits it to a cryptographic module of a document producer later on, at a different point in time from the transfer between the cryptographically reliable contact station and the intermediate station.

Therefore, the invention provides that the cryptographic module, also if it is supplied via an intermediate station, for example, via communication partners that are not reliable in the cryptographic sense – is provided with two types of data, one of which remains in the cryptographic module while the other is attached to the document, whereby the information remaining in the cryptographic module is used to secure the document information by means of a check value and whereby the information incorporated into the document, within the scope of a check of the genuineness of the document in a checking station, serves to substantiate that the document has been secured by means of the cryptographic module.

The invention comprises numerous advantages. It makes it possible to generate forgery-proof documents in a large number of application cases, especially in those cases where no direct connection exists between the document producer and the reliable contact station. For example, in this manner, forgery-proof documents can be generated without the use of computers and/or a data connection to the reliable contact station.

As a matter of principle, it is possible to select the key information according to a prescribed pattern. However, this facilitates cryptographic decrypting attacks (enigma problem).

It is especially advantageous for the key information to be formed by being generated randomly although the invention can be carried out with a predefinable set of key information. The random generation of the key information is especially advantageous since this makes it possible to avoid having to store large volumes of key information.

It has proven to be advantageous for the encrypted key information and/or the encrypted checking information to be configured in such a way that it cannot be decrypted in the intermediate station.

A decryption of the key information by the cryptographic module entails several advantages. In this way, a user of the cryptographic module, especially a document producer, can obtain a confirmation of having received information from the reliable contact station, especially monetary value information created by the reliable contact station. Moreover, in this fashion, the cryptographic module can use the received key information for a subsequent encryption.

A preferred use of the key information is for the encryption of the document producer's own data.

Advantageously, the document producer supplies his own data to the cryptographic module, preferably by an automated method.

An especially preferred embodiment of the invention is characterized in that the data entered by the document producer is irreversibly linked to the key information by means of the cryptographic module.

Here, it is especially advantageous for the data entered by the document producer and the decrypted key information to be irreversibly linked in that the key information is used to form a check value for the document.

Moreover, it is especially advantageous for the result of the irreversible linking of the data entered by the document producer with the decrypted key information to form a document and/or a data record that is transmitted to a checking station.

It has also proven to be advantageous for the document transmitted to the checking station to contain the document producer's own data at least partially in plain text.

For this purpose, it is especially advantageous for the encrypted checking information to be entered into the document that is transmitted to the checking station.

It is advantageous for the information remaining in the cryptographic module to be encrypted in such a way that it can be decrypted in the cryptographic module and for the information remaining in the cryptographic module to be a value that is difficult or impossible to predict.

It is especially advantageous for the supply of the cryptographic module via communication partners that are cryptographically not reliable to be carried out in such a way that an exchange of information within a dialog is not necessary.

It is likewise a special advantage that the supply of the cryptographic module via communication partners that are cryptographically non-reliable is carried out in such a way that the information is forwarded to the cryptographic module at a different point in time.

It has proven to be important and advantageous for the supply of the cryptographic module, also in case of a supply via communication partners that are cryptographically not reliable, to be carried out by a reliable station whose information can be relied on by the checking station.

REPLACED BY
ART 34 AMDT

Patent Claims:

1. A method for the generation of forgery-proof documents or data records, whereby key information is generated and whereby encrypted checking information is formed from the key information and from a transaction indicator, characterized in that
the generation of the random key information and the formation of the encrypted checking information from the key information and from the transaction indicator are carried out in a cryptographically reliable contact station, in that the cryptographically reliable contact station encrypts the key information, and in that the encrypted checking information and the encrypted key information are transmitted by the cryptographically reliable contact station to an intermediate station, in that the intermediate station temporarily stores the encrypted key information and the encrypted checking information and transmits it to a cryptographic module of a document producer later on, at a different point in time from the transfer between the cryptographically reliable contact station and the intermediate station.
2. The method according to Claim 1, characterized in that
the key information is generated in such a way that the key information is formed randomly.
3. The method according to one or more of the preceding claims, characterized in that
the encrypted key information and/or the encrypted checking information is configured in such a way that it cannot be decrypted in the intermediate station.
4. The method according to one or more of the preceding claims, characterized in that
the cryptographic module preferably decrypts the key information with a key contained in the cryptographic module.

5. The method according to one or more of the preceding claims, characterized in that
the document producer enters his own data into the cryptographic module.
6. The method according to one or more of the preceding claims, characterized in that
the data entered by the document producer is irreversibly linked to the key information by means of the cryptographic module.
7. The method according to Claim 6, characterized in that
the data entered by the document producer and the decrypted key information are irreversibly linked in that the key information is used to form a check value for the document.
8. The method according to one or both of Claims 6 or 7, characterized in that
the result of the irreversible linking of the data entered by the document producer with the decrypted key information forms a document and/or a data record that is transmitted to a checking station
9. The method according to Claim 8, characterized in that
the document transmitted to the checking station contains the document producer's own data, at least partially in plain text.
10. The method according to one or both of Claims 8 or 9, characterized in that
the encrypted checking information is entered into the document that is transmitted to the checking station.
11. The method according to one or more of the preceding claims, characterized in that
information remaining in the cryptographic module is encrypted in such a way that it can be decrypted in the cryptographic module.

12. The method according to one or more of the preceding claims, characterized in that
the supply of the cryptographic module with the information, also in case of a supply via communication partners that are not reliable in the cryptographic sense, is carried out by a cryptographically reliable station whose information can be relied on by the checking station.
13. The method according to Claim 12, characterized in that,
in order for a reliable station to provide reliable information for the cryptographic module, cryptographic encryptions are used that the checking station can reverse.
14. The method according to one or more of Claims ... to 13, characterized in that
the supply of the cryptographic module via communication partners that are cryptographically non-reliable is carried out in such a way that the information is forwarded to the cryptographic module at a different point in time.
15. The method according to one or more of Claims 1 to 14, characterized in that
the supply of the cryptographic module via communication partners that are cryptographically not reliable is carried out in such a way that an exchange of information within a dialog is not necessary.
16. The method according to one or more of Claims 1 to 14, characterized in that
the two types of data are cryptographically linked to each other, but cannot be discovered by means of crypto-analysis.
17. The method according to Claim 19, characterized in that
the cryptographic linking of the two types of data is such that non-linear fractions are added that are known only to the reliable contact station and to the checking station.

18. The method according to one or more of the preceding claims, characterized in that
the generated forgery-proof documents or data records contain monetary value information.
19. The method according to Claim 18, characterized in that
the monetary value information is cryptographically connected to the document or data record in such a way that a check value can be formed by comparing the monetary value information to the document or data record.
20. The method according to one or both of Claims 18 or 19, characterized in that
the monetary value information contains proof of the payment of postage amounts.
21. The method according to Claim 20, characterized in that
the monetary value information that proves the payment of postage amounts is linked to identification data of the document producer.
22. The method according to one or both of Claims 20 or 21, characterized in that
the monetary value information is linked to address data.
23. A value transfer center with an interface for loading monetary values, characterized in that
the value transfer center contains an interface to receive encrypted information of a cryptographically reliable contact station and to temporarily store the received encrypted information.
24. The value transfer center according to Claim 23, characterized in that
the information is encrypted in such a way that it cannot be decrypted in the value transfer center.

25. The value transfer center according to one or more of Claims 23 to 24, characterized in that it contains means for receiving value transfer requests by at least one cryptographic module and for forwarding the received encrypted information at a different point in time.
26. A cryptographic module for generating forgery-proof documents with means to issue encrypted checking information and a check value, characterized in that the cryptographic module contains at least one means for receiving and decrypting key information and at least one means for receiving a document or a data record, and in that the cryptographic module has at least one means to form a check value for the document or for the data record using the key information.